UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/775,205	02/01/2001	Alan Boate	RIDM.P-002	7111

32692 7590 06/16/2004

3M INNOVATIVE PROPERTIES COMPANY
PO BOX 33427
ST. PAUL, MN 55133-3427

EXAMINER	
SHIFERAW, ELENI A	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 06/16/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/775,205	BOATE ET AL.	
	Examiner	Art Unit	
	Eleni A Shiferaw	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02/01/2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-22* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *02/01/2001*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-22 are presented for examination.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1, 3, 5, 6, 7, 8, and 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Maritzen et al. (Maritzen, U.S. Pub. No. US 2002/0073042 A1) in view of DeLaHuerga (U.S. Patent No. 6,408,330 B1)

4. As per claim 1, a personal digital identifier device (Page 1-2 par. 0032; transaction device which has a unique identifier comprising privacy card and digital wallet) for controlling access to a computer network, said network comprising a plurality of workstations each having a base unit associated therewith, said base unit being configured for wireless communications with said personal digital identifier device (Page 19 par. 0250; wireless base station), and said network further comprising a central server utilizing a security manager component and network storage (Page 5 par. 0063; TPCH embodied as a secure server for authentication), said security manager component associated with a private key and a corresponding public key and a public key corresponding to a private key held by said personal digital identifier device (Page 2 par. 0039, page 11 par. 0157; PKI and private key respectively), said personal digital identifier device being

lightweight, configured for wearing and/or carrying by a user registered thereto (Page 6 par. 0082; easy sized carrying privacy card) and comprising:

(a) a wireless communications component comprising a transceiver for communicating with said base unit; (Page 3 par. [0041-0043], page 14 par. [0184-0185], fig. 9, and fig. 14)

(b) a biometric acquisition component for obtaining a user's input biometric and producing a digital representation thereof; (Page 2 par. 0038, page 19 par. 0251, page 20 par. 0259, fig. 7c, and 21)

(c) a processor configured for communicating with said transceiver and said biometric component and operable for: (Page 14 par. [0184-0185], page 8 par. 0103)

(i) evaluating whether a template derived from said digital representation corresponds to a master template derived from a user's biometric digital representation previously produced by said biometric component and generating a matching signal when such a correspondence is determined; (Page 2 par. [0038-0043], page 8 par. 0103])

(ii) generating said private key held by said personal digital identifier device and said public key corresponding thereto and outputting said generated public key for transmission by said transceiver; (Page 11 par. 0157)

(iii) producing a digital signature using said private key; (Page 11-12 par. [0157-0167])

and,

(iv) verifying, using said public key for said private key associated with said security manager component, that the source of an encrypted message ostensibly received from said security manager is said security manager component; (Page 2 par. 0039)

(e) a power source; (Page 6 par. 0079; temporary battery, page 7 par. 0091, page 8 par. 0109, and fig. 14) and,

(f) a housing, (Fig. 8)

said personal digital identifier device being configured for producing, using said generated private key, (Page 11 par. 0157, Fig. 6) a digitally signed challenge response message following said generating of said matching signal in response to a challenge message received from said security manager component and for transmitting said response message, (Page 5 par. [0066-0068]) and said personal digital identifier device being configured to prevent transmission of any of said master template of a user's biometric (Page 2 par 0038, page 8 par. 0103 page 19 par. 0251, and fig. 21) and said private key. (Page 11 par. 0157)

Maritzen fails to explicitly describe secure storage.

However, DeLaHuerga teaches matching the original document with the signature picture in associated with private key and public key for authentication. (Col. 8 lines 19-27,Col. 15 lines 36-45, Col. 23 lines 1-13, Col. 30 lines 63-col 31 lines 45)

Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to combine the teachings of DeLaHuerga with Martizen to contain the master template of a user's biometric, the generated private key and the public key for the private key associated with said security manager component in the secure storage, to authenticate the content and signature of the document using public key and private key.

5. As per claim 3, the combination of Maritzen and DeLaHuerga teach the subject matter claimed above. In addition Maritzen teaches personal digital identifier device wherein a response signal is automatically transmitted from said transceiver in response to a signal received by said transceiver from one said base unit. (Page 7 par. 0091, page 17 par. 0221, page 20 par. 0256, fig. 21)

6. As per claim 5, the combination of Maritzen and DeLaHuerga teach the subject matter claimed above. In addition Maritzen teaches a personal digital identifier device wherein said transducer comprises a solid state 'fingerprint sensor. (Page 3 par. 0043, page 6 par. [0080-0085])

7. As per claim 6, the combination of Maritzen and DeLaHuerga teach the subject matter claimed above. In addition Maritzen teaches a personal digital identifier device wherein said transceiver transmits and receives optical signals. (Page 8 par. 0111)

8. As per claim 7, the combination of Maritzen and DeLaHuerga teach the subject matter claimed above. In addition Maritzen teaches a personal digital identifier device wherein said transceiver transmits and receives radio frequency signals. (Page 6 par. 0079-0080)

9. As per claim 8, the combination of Maritzen and DeLaHuerga teach the subject matter claimed above. In addition Maritzen teaches a personal digital identifier device in combination

with a device holder wherein said device holder is configured to co-operate with said housing of said personal digital identifier device such that said personal digital identifier device is held by said holder device when it is appropriately positioned relative to said holder device, said device holder comprising a communications connector for communicatively coupling said personal digital identifier device directly to one said workstation when said personal digital identifier device is held by said device holder. (Fig. 8, 9a, 9b; digital wallet and privacy card, page 1-2 par. 0032, and 0038)

10. As per claim 13, the combination of Maritzen and DeLaHuerga teach the subject matter claimed above. In addition Maritzen teaches a security system comprising a plurality of said personal digital identifier devices, a plurality of workstations and a plurality of base units wherein a base unit is associated with each said workstation, each said base unit transmitting a polling signal to each said personal digital identifier device within said base unit's associated envelope following said base unit's receipt of said response signal from each said personal digital identifier device. (Page 15 par. 0202, page 19 par. 0251)

11. Claims 2, 4, 9, 10, 11, 12, 14, and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Maritzen et al. (Maritzen, U.S. Pub. No. US 2002/0073042 A1) in view of DeLaHuerga (U.S. Patent No. 6,408,330 B1) and in further view of Gainsboro et al. (Gainsboro, U.S. Pub. 2001/0036821 A1)

12. As to claim 9, it has similar limitations as claim 1; therefore, it is being rejected under the same rationale over Maritzen and DeLaHuerga. In addition, DeLaHuerga teaches a server having access to network storage to authenticate a user that reads on a central server having access to network storage and utilizing said security manager component and said personal digital identifier device for authenticating said user, said network storage containing a public key corresponding to said private key generated by said personal digital identifier device. (Col. 47 lines 9-43)

DeLaHuerga fails to teach the communications extending over an area defined by an envelope associated with said workstation.

However, Gainsboro teaches a base unit associated with said workstation and configured for initiating and maintaining wireless communications with identifier device, the communications extending over an area defined by an envelope associated with said workstation; (Page 6 par. 0062, Fig. 5-6)

It would have been obvious to one having ordinary skill in the art at the time the invention was made to combine the teachings of Maritzen and Gainsboro to intercept the transmission of wireless communication signals in order to provide wireless communications control and to achieve improved security.

13. As per claims 2 and 10, the combination of Maritzen, DeLaHuerga, and DeLaHuerga teach the subject matter claimed above. In addition Maritzen teaches a personal digital identifier device (system) wherein said biometric component includes a transducer. (Page 3 par. 0043, page 6 [0080-0085]; fingerprint recognition built in the card.)

14. As per claims 4 and 14, the combination of Maritzen, DeLaHuerga, and Gainsboro teach the subject matter claimed above. In addition Maritzen teaches a personal digital identifier device wherein all data held in said secure storage is by itself non-identifiable of said user. (Page 1-2 par. 0032, par. 0037, page 5 par. 0074, page 11 par. 0152, page 14 par. 0190)

15. As per claim 11, the combination of Maritzen, DeLaHuerga, and Gainsboro teach the subject matter claimed above. In addition Maritzen teaches a security system wherein said workstation is a personal computer. (Page 3 par. 0041, page 19 par. 0252)

16. As per claim 12, the combination of Maritzen, DeLaHuerga, and Gainsboro teach the subject matter claimed above. In addition Maritzen teaches a security system wherein said base unit regularly transmits a first signal to said personal digital identifier device and said personal digital identifier device automatically transmits a response signal in response. (Page 19 par. 0250)

17. As per claim 16, the combination of Maritzen, DeLaHuerga, and Gainsboro teach the subject matter described above. In addition Gainsboro discloses security system wherein said envelope has a shape and area which are configured to encompass those locations proximate to said workstation at which an observer may read and/or understand information displayed on a screen of said workstation. (Fig. 4, Page 6 par. 0058) The rational for combining are the same as claim 9 above.

Claim Rejections - 35 USC § 103

18. Claim 15 is rejected under 35 U.S.C. 103(a) as being unpatentable over Maritzen et al. (Maritzen, U.S. Pub. No. US 2002/0073042 A1) in view of DeLaHuerga (U.S. Patent No. 6,408,330 B1), Gainsboro et al. (Gainsboro, Pub No. U.S. 2001/0036821) in further view of Blumenau et al. (Blumenau, Pub. No. U.S. 2001/0020254 A1)

19. As per claim 15, the combination of Maritzen, DeLaHuerga, and Gainsboro teach the subject matter described above.

Maritzen, DeLaHuerga, and Gainsboro fail to explicitly disclose network storage of a security system.

However, Blumenau discloses security system wherein said network storage includes data identifiable of said user for display on a screen of said workstation when identification device is located.

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to combine the teachings of Blumenau with the combination of Maritzen, DeLaHuerga, and Gainsboro to manage access to a storage system by a plurality of devices that are coupled to the storage system via a network and to secure data.

Claim Rejections - 35 USC § 103

20. Claims 17, 18, 19, 20, 21, and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over (Maritzen, U.S. Pub. No. US 2002/0073042 A1) in view of DeLaHuerga (U.S.

Patent No. 6,408,330 B1), Gainsboro et al. (Gainsboro, Pub No. U.S. 2001/0036821), Blumenau et al. (Blumenau, Pub. No. U.S. 2001/0020254 A1), and in further view of Atsmon et al. (Atsmon, U.S. 6,607,136 B1)

21. As per claim 17 the combination of Maritzen, DeLaHuerga, Gainsboro, and Blumenau teach the subject matter. Maritzen, DeLaHuerga, Gainsboro, and Blumenau fail to explicitly describe the method steps for access control.

However, Atsmon teaches the method comprising the steps:

(a) on registration of a portable personal digital identifier device to a user, within said portable personal digital identifier device: Col. 15 lines 23-40) receiving an input biometric of said user, (Col. 86 lines 17-43) producing a digital representation thereof, (Col. 86 lines 17-43, Col. 102 lines 26-43) deriving from said digital representation a master template, (Col. 102 lines 26-43) securely maintaining said master template in storage, (Col. 58 lines 63- col. 59 lines 13) generating and securely maintaining in said storage a private key, (Col. 83 lines 20-33) generating a public key corresponding to said generated private key (Col. 84 lines 23-41) and providing said generated public key for storage in said network storage (Col. 84 lines 23-50) and receiving and storing in said storage a public key for a private key associated with a network security manager component; (Col. 85 lines 66-col. 87 lines 20)

(b) transmitting a first signal from a base unit associated with one said workstation to said personal digital identifier device and automatically transmitting from said

personal digital identifier device a response signal establishing communications between said base unit and said personal digital identifier device in response to said first signal when said personal digital identifier device is within said envelope; (Abstract, Col. 23 lines 46-57, Col. 8 lines 37-Col. 9 lines66, Fig. 1, 37-39)

(c) receiving at said personal digital identifier device a digitally signed challenge message ostensibly from said network security manager component and verifying within said personal digital identifier device the origin of said challenge using said public key for said private key associated with said security manager component; (Col. 86 lines 44-col. 87 lines 9)

(d) acquiring on said portable personal digital identifier device an input biometric of said user, producing a digital representation thereof and deriving from said digital representation a biometric template; (Col. 86 lines 36-44)

(e) evaluating within said portable personal digital identifier device whether said biometric template corresponds to said master template and generating a matching signal when such a correspondence is determined; (Col. 45 lines 16-30, Col. 591-13)

(f) producing within said personal digital identifier device, using said generated private key, a digitally signed challenge response message following said generating of said matching signal in response to said challenge message and transmitting said response message to said security manager component to authenticate said user; and, (Col. 85 lines 66- col. 87 lines 8)

(g) permitting said authenticated user to access said computer network through said workstation. (Col. 2 lines 13-24, Col. 32 lines 51-64)

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to combine the teachings of Atsmon in the combination of Maritzen, DeLaHuerga, Gainsboro, and Blumenau to provide a secure authentication in a manner where the functionality associated with the card is accessed via a public network such as the Internet, and to enhance security in using biometric analysis.

22. As per claim 18, a method according to claim 17 and further comprising configuring the shape and area of said envelope to encompass those locations proximate to said workstation at which an observer may read and/or understand information displayed on a screen of said workstation. (Fig. 24, Col. 10 lines 51-59, 48 lines 43-col. 49 lines 23) The rational for combining are the same as claim 17 above.

23. As per claim 19, a method according to claim 17 and further comprising, following said base unit's receipt of said response signal from said personal digital identifier device, transmitting from said base unit a polling signal to said personal digital identifier device for determining whether said personal digital identifier device remains located within said base unit's associated envelope. (Col. 10 lines 51-59) The rational for combining are the same as claim 17 above.

24. As per claim 20, a method according to claim 17 and further comprising displaying on a screen of said workstation data identifying said user when said user is identified. (Col. 18 lines 62-Col. 19 lines 12, Page 78 lines 39-62) The rational for combining are the same as claim 17 above.

25. As per claim 21, a method according to claim 17 and further comprising initially registering said user by a registrar in the presence of a guarantor, (Col. 68 lines 53-67) said registrar and guarantor each being a registered user of the computer network and said registrar having access to the computer network and verified by said security manager component to have registration privileges, (Col. 102 lines 26-41) and requiring: that said guarantor provide to said security manager component a biometrically digitally signed message to authenticate said guarantor and that each of said registrar, guarantor and user remain within said envelope during said registering of said user. (Col. 102 lines 26-41) The rational for combining are the same as claim 17 above.

26. As per claim 22, a method according to claim 17 whereby a policy manager component may direct that the screen of said workstation be blanked out when a new personal digital identifier device moves to a location within said envelope until such time as the user registered to said personal digital identifier device is biometrically identified. (Col. 35 lines 35-50) The rational for combining are the same as claim 17 above.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Eleni A Shiferaw whose telephone number is 703 305 0326. The examiner can normally be reached on Mon-Fri 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R Sheikh can be reached on 703 305 9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Eleni Shiferaw
Art Unit 2136

AYAZ SHEIKH
PATENT EXAMINER
TECHNOLOGY CENTER 2100

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100